

1118.70214

PATENT

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Applicant: Li et al.

Serial No. 10/811,323

Conf. No. 9463

Filed: March 26, 2004

For: DIGITAL SIGNATURE GENERATION )  
METHOD, DIGITAL SIGNATURE )  
AUTHENTICATION METHOD, )  
DIGITAL SIGNATURE GENERATION )  
REQUEST PROGRAM AND DIGITAL )  
SIGNATURE AUTHENTICATION )  
REQUEST PROGRAM )

Art Unit: 2131 )

Examiner: Unassigned )



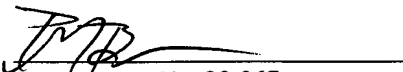
I hereby certify that this paper is being deposited with the United States Postal Service as FIRST-CLASS mail in an envelope addressed to: Mail Stop MISSING PARTS, Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450, on this date.

August 9, 2004

Date

F-CLASS.WCM

Appr. February 20, 1998

  
Registration No. 29,367

Attorney for Applicant

**CLAIM FOR PRIORITY**

Mail Stop MISSING PARTS  
Commissioner for Patents  
P.O. Box 1450  
Alexandria, VA 22313-1450

Dear Sir:

Applicants claim foreign priority benefits under 35 U.S.C. § 119 on the basis of the foreign application identified below:

Japanese Patent Application No. 2003-092280, filed March 28, 2003.

A certified copy of the priority document is enclosed.

Respectfully submitted,

GREER, BURNS & CRAIN, LTD.

Customer No. 24978

August 9, 2004  
300 South Wacker Drive  
Suite 2500  
Chicago, Illinois 60606  
Tel: (312) 360-0080  
Fax: (312) 360-9315

By



Patrick G. Burns  
Registration No. 29,367

日 本 国 特 許 庁  
JAPAN PATENT OFFICE

別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed with this Office.

出 願 年 月 日      2 0 0 3 年   3 月 2 8 日  
Date of Application:

出 願 番 号      特 願 2 0 0 3 - 0 9 2 2 8 0  
Application Number:  
[ST. 10/C]:      [ J P 2 0 0 3 - 0 9 2 2 8 0 ]

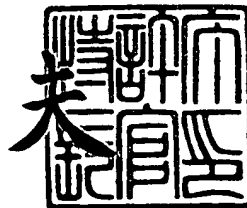
出 願 人      富士通株式会社  
Applicant(s):

CERTIFIED COPY OF  
PRIORITY DOCUMENT

2 0 0 3 年 1 2 月   8 日

特許庁長官  
Commissioner,  
Japan Patent Office

今 井 康 夫



出証番号   出証特 2 0 0 3 - 3 1 0 1 3

【書類名】 特許願

【整理番号】 0252392

【あて先】 特許庁長官 殿

【国際特許分類】 G09C 1/00 640

【発明の名称】 電子署名生成方法，電子署名検証方法，電子署名生成依頼プログラム，及び電子署名検証依頼プログラム

【請求項の数】 4

【発明者】

【住所又は居所】 神奈川県川崎市中原区上小田中 4 丁目 1 番 1 号 富士通株式会社内

【氏名】 李 濤

【発明者】

【住所又は居所】 神奈川県川崎市中原区上小田中 4 丁目 1 番 1 号 富士通株式会社内

【氏名】 小泉 潤一

【発明者】

【住所又は居所】 神奈川県川崎市中原区上小田中 4 丁目 1 番 1 号 富士通株式会社内

【氏名】 加藤 広己

【発明者】

【住所又は居所】 神奈川県横浜市港北区新横浜二丁目 4 番地 1 9 株式会社富士通ハイパーソフトテクノロジー内

【氏名】 宮崎 達弘

【特許出願人】

【識別番号】 000005223

【氏名又は名称】 富士通株式会社

## 【代理人】

【識別番号】 100098235

## 【弁理士】

【氏名又は名称】 金井 英幸

## 【手数料の表示】

【予納台帳番号】 062606

【納付金額】 21,000円

## 【提出物件の目録】

【物件名】 明細書 1

【物件名】 図面 1

【物件名】 要約書 1

【包括委任状番号】 9908696

【プルーフの要否】 要

【書類名】 明細書

【発明の名称】 電子署名生成方法，電子署名検証方法，電子署名生成依頼プログラム，及び電子署名検証依頼プログラム

【特許請求の範囲】

【請求項 1】

ネットワークを介して端末とサーバ装置とが通信可能に構成されているシステム上において、前記端末の記憶部内に存在している電子情報に対する電子署名を生成するための電子署名生成方法であって、

前記端末が、前記電子情報のダイジェスト値を算出し、

前記端末が、前記ダイジェスト値、及び、前記電子情報の発行元が有する識別情報を、前記サーバ装置へ送信し、

前記サーバ装置が、予め各識別情報毎に秘密鍵及び公開鍵を対応付けて格納している記憶装置から、前記端末から受信した識別情報に対応する秘密鍵を取り出し、

前記サーバ装置が、前記端末から受信したダイジェスト値を前記記憶装置から取り出した秘密鍵によって暗号化することによって署名値を生成し、

前記サーバ装置が、生成した署名値を前記端末へ応答し、

前記端末が、前記サーバ装置から応答された署名値及び前記識別情報を前記電子情報に添付することによって電子署名付き電子情報を構成することを特徴とする電子署名生成方法。

【請求項 2】

ネットワークを介して端末とサーバ装置とが通信可能に構成されているシステム上において、請求項 1 記載の電子署名生成方法によって得られた電子署名付き電子情報を検証するための電子署名検証方法であって、

前記端末が、前記電子署名付き電子情報中の電子情報のダイジェスト値を算出し、

前記端末が、前記ダイジェスト値、並びに、前記電子署名付き電子情報中の前記署名値及び前記識別情報を、前記サーバ装置へ送信し、

前記サーバ装置が、前記端末から受信した識別情報に対応する公開鍵を前記記

憶装置から取り出し、

前記サーバ装置が、前記端末から受信した署名値を前記記憶装置から取り出した公開鍵によって復号化し、

前記サーバ装置が、復号化した前記署名値の内容と前記端末から受信したダイジェスト値とが一致しているか否かを比較し、

前記サーバ装置が、前記比較の結果を前記端末へ応答することを特徴とする電子署名検証方法。

### 【請求項 3】

予め各識別情報毎に秘密鍵及び公開鍵を対応付けて記憶する記憶装置を有するとともに、暗号化対象情報及び識別情報を指定した電子署名生成依頼メッセージを受信した時には、受信した識別情報に対応する秘密鍵を前記記憶装置から取り出し、取り出した秘密鍵によって前記暗号化対象情報を暗号化することによって署名値を生成し、生成した署名値を応答するサーバ装置との間で、ネットワークを通じて通信可能なコンピュータに対して、

電子情報及び当該電子情報の発行元の識別情報が入力された場合には、

前記電子情報のダイジェスト値を算出させ、

算出されたダイジェスト値を前記暗号化対象情報として前記識別情報とともに指定した電子署名生成依頼メッセージを、前記サーバ装置へ送信させ、

前記サーバ装置から前記署名値が応答された場合には、

当該署名値及び前記識別情報を前記電子情報に添付することによって電子署名付き電子情報を構成させる

ことを特徴とする電子署名生成依頼プログラム。

### 【請求項 4】

予め各識別情報毎に秘密鍵及び公開鍵を対応付けて記憶する記憶装置を有するとともに、検証対象情報、署名値及び識別情報を指定した電子署名検証依頼メッセージを受信した時には、受信した識別情報に対応する公開鍵を前記記憶装置から取り出し、取り出した公開鍵によって前記署名値を復号化し、復号化された署名値と前記検証対象情報とが一致しているか否かを比較して、比較結果を応答するサーバ装置との間で、ネットワークを通じて通信可能なコンピュータに対して

、  
前記請求項 1 又は 3 に従って得られた電子署名付き電子情報が入力された場合には、

前記電子署名付き電子情報中の電子情報のダイジェスト値を算出させ、

当該ダイジェスト値を前記検証対象情報として前記電子署名付き電子情報中の前記署名値及び前記識別情報とともに指定した電子署名検証依頼メッセージを、前記サーバ装置へ送信させる

ことを特徴とする電子署名検証依頼プログラム。

#### 【発明の詳細な説明】

##### 【0 0 0 1】

#### 【発明の属する技術分野】

本発明は、ネットワークを介して複数の利用者端末とサーバ装置とが通信可能に構成されているシステム上において、何れかの利用者端末内に存在している電子情報に対する電子署名を生成するための電子署名生成方法、このような電子署名生成方法に従って生成された電子署名を検証するための電子署名検証方法、電子署名生成機能を有するサーバ装置と通信可能なコンピュータに上記電子署名生成方法を実施させる電子署名生成依頼プログラム、及び、電子署名検証機能を有するサーバ装置と通信可能なコンピュータに上記電子署名検証方法を実施させる電子署名検証依頼プログラムに、関する。

##### 【0 0 0 2】

#### 【従来の技術】

従来、電子情報の暗号化及び電子署名の方法として、R S A 公開鍵方式が知られている。この R S A 公開鍵方式とは、一方の鍵を用いて暗号化された電子情報は他方の鍵を用いなければ復号化できないという関係にある鍵ペアを生成し、そのうちの一つを秘密鍵として非公開とするとともに、他の一つを公開鍵として第三者に公開する方式である。そして、電子署名をする際には、署名対象電子情報をその発行者固有の秘密鍵によって暗号化して電子署名を生成し、この電子署名を暗号化前の署名対象電子情報（以下、「平文の署名対象電子情報」という）に添付して、当該電子情報の相手方へ渡す。この電子署名付きの電子情報を受け取

った相手方は、その電子情報の発行者のものとして公開されている公開鍵を用いて電子署名を復号化し、復号化によって再現された電子情報と平文の電子情報とを照合し、両者が一致していれば、その平文の電子情報が真正なものであると判断することができ、両者が一致していなければ、その平文の電子情報が真正なものではない（即ち、表示された発行者以外の者によって偽造されたか、第3者によって改竄されたものである）と判断することができる。

#### 【0 0 0 3】

【特許文献1】 特開 2 0 0 2 - 3 3 7 6 0 号公報

#### 【0 0 0 4】

以上のような電子署名の生成及び電子署名の検証は、電子情報を発行する者及び電子情報を受け取った者が自らが管理する端末上で行うのが基本であるが、ネットワークを通じてこれらの者から電子署名の作成及び検証の依頼を受けてこれらの作業を代行するサービスも、実施されている。このような代行サービスを行うサービス提供者が運営するサーバ装置は、契約を取り交わした各利用者の鍵ペアを予め登録しておき、何れかの利用者が操作する端末から電子署名作成依頼及び署名対象電子情報をネットワーク経由で受け取ると、その利用者の秘密鍵によって当該署名対象電子情報を暗号化して電子署名を生成し、生成した電子署名を依頼元利用者が操作する端末へ返送する。依頼元利用者は、サーバ装置から受け取った電子署名を平文の署名対象電子情報に添付して、当該電子情報の相手方へ渡す。この電子署名付きの電子情報を受け取った相手方は、これら平文の電子情報及び電子署名をネットワーク経由で自ら操作する端末からサーバ装置へ送信し、電子署名の検証を依頼する。検証依頼を受けたサーバ装置は、その電子署名の発行者のものとして登録されている公開鍵によって電子署名を復号化し、復号化によって再現された電子情報と平文の電子情報とを照合し、両者が一致していれば、その平文の電子情報が真正なものである旨を依頼者操作の端末へ応答し、両者が一致していなければ、その平文の電子情報が真正なものではない旨を依頼者操作の端末へ応答する。

#### 【0 0 0 5】

【発明が解決しようとする課題】



しかしながら、従来の電子署名生成方法及び電子署名検証方法によると、各個人が管理する端末上において電子署名の生成又は検証を行う場合であっても、電子情報の発行者又は相手方から依頼を受けたサーバ装置上において電子署名の生成又は検証を行う場合であっても、夫々、以下のような問題がある。

#### 【 0 0 0 6 】

すなわち、各個人が管理する端末上において電子署名の生成及び検証を行う場合には、その個人は、自己の鍵ペア、特に秘密鍵を、紛失することが無い様、また、他人に漏洩してしまうことが無い様、維持及び管理しなければならない、また、自ら電子署名の作成及び検証をしなければならない。そのため、その個人は、鍵の生成、維持管理、電子署名の作成、電子署名の検証を行うためのソフトウェアを、端末のハードウェアに加えて、導入しなければならない。よって、その個人は、これらソフトウェア及びハードウェアの導入及び維持コストや運用管理コストを負担しなければならないのみならず、運用ノウハウを自ら蓄積するか他者から提供されなければならない。

#### 【 0 0 0 7 】

また、ネットワーク上のサーバ装置上において電子署名の生成及び検証を行う場合には、電子署名の作成を依頼する利用者は、平文の電子情報をネットワーク経由でサーバ装置へ送らねばならない。また、電子署名の検証を依頼する利用者は、電子署名に添付して平文の電子情報をネットワーク経由でサーバ装置へ送らねばならない。これら利用者が操作する端末とサーバ装置との間においては、実装の普及している S S L (Secure Socket Layer) を使用すれば、第三者による不正アクセスは或る程度防止することができる(また、電子署名を添付した電子情報を発行者と相手方との間で交換する間も、R S A 公開鍵暗号化アルゴリズム等の暗号化技術を利用することによって第三者による不正アクセスを防止することができる)。しかしながら、サーバ装置内においては、暗号化前又は復号化後の電子情報は平文であるので、このサーバ装置を運営するサービス提供者に対して電子情報の内容を隠すことができない。

#### 【 0 0 0 8 】

本発明は、以上のような問題点に鑑みてなされたものであり、電子署名の作成

又は検証をネットワーク上のサーバ装置上において代行することによって各個人の負担を軽減することができるとともに、署名対象電子情報そのものをサーバ装置において暗号化又は復号化することなく電子署名として機能する暗号化情報を作成し、また、署名対象電子情報の検証を行うことができる電子署名作成方法及び電子署名検証方法、電子署名生成機能を有するサーバ装置と通信可能なコンピュータに上記電子署名生成方法を実施させる電子署名生成依頼プログラム、並びに、電子署名検証機能を有するサーバ装置と通信可能なコンピュータに上記電子署名検証方法を実施させる電子署名検証依頼プログラムの提供を、課題とする。

#### 【0009】

##### 【課題を解決するための手段】

上記課題を解決するために案出された本発明による電子署名生成方法によると、署名対象電子情報の発行元が操作する発行元端末は、署名対象電子情報のダイジェスト値を算出し、このダイジェスト値、及び、署名対象電子情報の発行元が有する識別情報を、サーバ装置へ送信する。すると、サーバ装置は、予め各識別情報毎に秘密鍵及び公開鍵を対応付けて格納している記憶装置から、発行元端末から受信した識別情報に対応する秘密鍵を取り出し、発行元端末から受信したダイジェスト値を記憶装置から取り出した秘密鍵によって暗号化することによって署名値を生成し、生成した署名値を発行元端末へ応答する。すると、発行元端末は、サーバ装置から応答された署名値及び識別情報を署名対象電子情報に添付することによって、電子署名付き電子情報を構成する。

#### 【0010】

また、上記課題を解決するために案出された本発明による電子署名検証方法によると、発行元から電子署名付き電子情報を受け取った相手方が操作する相手方端末は、この電子署名付き電子情報中の電子情報のダイジェスト値を算出し、このダイジェスト値、並びに、前記電子署名付き電子情報中の署名値及び識別情報をサーバ装置へ送信し、相手方端末から受信した識別情報に対応する公開鍵を記憶装置から取り出し、相手方端末から受信した署名値を前記記憶装置から取り出した公開鍵によって復号化し、復号化した署名値の内容と相手方端末から受信したダイジェスト値とが一致しているか否かを比較し、比較の結果を相手方端末へ

応答する。

**【 0 0 1 1 】**

このように構成される本発明による電子署名生成方法及び電子署名検証方法によれば、電子署名の実体である署名値は、署名対象電子情報そのものではなく、発行元端末内において署名対象電子情報に基づいて算出されたダイジェスト値をサーバ装置内において暗号化することによって生成された値である。従って、本発明によれば、電子署名の生成及び検証をネットワーク上のサーバ装置上において代行することによって利用者の負担を軽減することができるにも拘わらず、電子署名の作成時においても検証時においても、署名対象電子情報そのものはサーバ装置内に存在しないので、その内容がサーバ装置の管理運営者に知られることがない。

**【 0 0 1 2 】**

なお、本発明による電子署名生成依頼プログラムは、上記発行元端末としてのコンピュータに対して、電子情報及び当該電子情報の発行元の識別情報が入力された場合には、前記電子情報のダイジェスト値を算出させ、算出されたダイジェスト値を前記暗号化対象情報として前記識別情報とともに指定した電子署名生成依頼メッセージを、前記サーバ装置へ送信させ、前記サーバ装置から前記署名値が応答された場合には、当該署名値及び前記識別情報を前記電子情報に添付することによって電子署名付き電子情報を構成させるプログラムである。

**【 0 0 1 3 】**

また、本発明による電子署名検証依頼プログラムは、上記相手方端末としてのコンピュータに対して、上記電子署名付き電子情報が入力された場合には、前記電子署名付き電子情報中の電子情報のダイジェスト値を算出させ、当該ダイジェスト値を前記検証対象情報として前記電子署名付き電子情報中の前記署名値及び前記識別情報とともに指定した電子署名検証依頼メッセージを、前記サーバ装置へ送信させるプログラムである。

**【 0 0 1 4 】**

**【発明の実施の形態】**

以下、図面に基づいて、本発明の実施の形態を説明する。本実施形態における

署名対象電子情報はXML文書であるので、以下、「署名対象コンテンツ」と称する。

#### 【0015】

図1は、本発明による電子署名生成方法及び電子署名検証方法を実施するための電子署名システムの概略構成を示すブロック図である。この電子署名システムは、電子署名代行サービス業者が管理運営する一台のサーバ装置（認証センターサーバ装置）1と、この電子署名代行サービス業者と電子署名代行についての契約を取り交わしている複数の利用者が夫々使用する複数の利用者端末2（図1においては1台のみ図示）とが、ネットワークNを介して互いに通信可能に接続されることにより、構成されている。なお、このネットワークNとしては、例えば、インターネットが利用可能であり、その場合には、認証センターサーバ装置1と各利用者端末2との間の通信は、HTTP（Hyper Text Transfer Protocol）に従ってなされる。

#### 【0016】

認証センターサーバ装置1は、ネットワークサーバ機能を有するコンピュータであり、そのハードウェアは、装置全体を制御するCPU（Central Processing Unit）10と、このCPU10に対してバスBを介して接続された通信部11、RAM（Random Access Memory）12及びHDD（Hard Disk Drive）13とから、構成されている。このうち、通信部11は、HDD13に格納されてCPU10によって実行されるプログラム（デバイスドライバ）によって制御され、ネットワークNとのインターフェースをなす通信アダプタである。また、RAM12は、CPU10によって用いられる作業領域が展開される主記憶装置である。

#### 【0017】

また、HDD13は、各種プログラム及び各種データを格納する記憶装置としてのコンピュータ可読媒体である。このHDD13が格納する各種プログラムには、上述したデバイスドライバや通信機能を有する基本プログラムであるOS（Operation System）の他、後においてフローチャートを用いて説明する電子署名代行プログラムが含まれている。この電子署名代行プログラムは、CPU10に

対して、各利用者端末 2 から送信されてきた電子署名代行依頼（署名対象コンテンツ及び当該利用者端末 2 を使用する利用者固有の鍵 ID を含む）に応じて電子署名生成を行わせ、また、各利用者端末 2 から送信されてきた電子署名検証依頼（署名対象コンテンツ、電子署名の実体である署名値及び当該利用者端末 2 を使用する利用者固有の鍵 ID を含む）に応じて電子署名検証を行わせるプログラムであり、RAM 12 上に読み出される署名生成部 121、署名検証部 122 及び鍵管理部 123 の各モジュールから、構成されている。署名生成部 121 は、電子署名生成を行うモジュールであり、署名検証部 122 は、電子署名検証を行うモジュールであり、鍵管理部 123 は、署名生成部 121 又は署名検証部 122 によって呼び出されて指定された利用者の秘密鍵又は公開鍵を検索するモジュールである。

#### 【0018】

また、HDD 13 が格納する各種データには、各利用者について予め生成された鍵ペア（秘密鍵及び公開鍵）を格納するためのテーブルである鍵格納庫 131 が含まれている。この鍵格納庫 131 は、具体的には図 2 に示すデータ構造を有しており、各利用者毎に、その利用者に対して予め通知されている識別情報（鍵 ID）及びパスワード（PW）の組、並びに、秘密鍵及び公開鍵を 1 レコードに登録することにより、構成されている。

#### 【0019】

一方、各利用者端末 2 は、ネットワークアクセス機能を有する一般的なパーソナルコンピュータであり、そのハードウェアは、装置全体を制御する CPU（Central Processing Unit）20 と、この CPU 20 に対してバス B を介して接続された通信部 21、RAM 22、HDD 23、ディスプレイ 24 及び入力装置 25 とから、構成されている。このうち、通信部 21 は、HDD 23 に格納されて CPU 20 によって実行されるプログラム（デバイスドライバ）によって制御され、ネットワーク N とのインターフェースをなす通信アダプタである。また、RAM 22 は、CPU 20 によって用いられる作業領域が展開される主記憶装置である。また、入力装置 25 は、利用者に属する担当者によって操作されることによって、CPU 20 に各種情報を入力するキーボード、ポインティングデバイス

等である。また、ディスプレイ 24 は、CPU 10 によって生成された各種画面を表示するための表示装置である。

#### 【0020】

また、HDD 23 は、各種プログラム及び各種データを格納するコンピュータ可読媒体である。この HDD 23 が格納する各種プログラムには、上述したデバイスドライバや通信機能を有する基本プログラムである OS (Operation System) の他、署名対象コンテンツを生成するアプリケーションプログラムや、後においてフローチャートを用いて説明する電子署名依頼プログラムが含まれている。この電子署名依頼プログラムは、CPU 20 に対して、アプリケーションプログラムが記憶部としての RAM 22 上で生成した署名対象コンテンツ又は記憶部としての RAM 22 上に取り込まれた署名対象コンテンツに対する電子署名代行依頼を認証センターサーバ装置 1 へ送信させ、また、通信部 21 又は図示せぬリムーバブル記憶媒体から RAM 22 上に取り込まれた電子署名付きコンテンツの検証依頼を認証センターサーバ装置 1 へ送信させるプログラムであり、RAM 22 上に読み出されるコンテンツ構成部 221 及び Digest 値計算部 222 の各モジュールを、含んでいる。コンテンツ構成部 221 は、認証センターサーバ装置 1 に対して電子署名作成依頼を行ってその結果として応答された署名値 (電子署名) に署名対象電子情報及び鍵 ID を添付して XML (Extended Markup Language) ファイル形式の電子署名付きコンテンツ (電子情報) として構成するとともに、認証センターサーバ装置 1 に対して電子署名検証依頼を行ってその結果として応答される検証結果をディスプレイ 24 に表示させるモジュールである。Digest 値計算部 222 は、コンテンツ構成部 221 によって呼び出され、指定された署名対象コンテンツ (XML 文書) の Digest 値 (ハッシュ値) を算出するモジュールである。

#### 【0021】

以下、上述した利用者端末 1 上での電子署名依頼プログラムによる処理及び認証センターサーバ装置 2 上での電子署名代行プログラムによる処理を、電子署名生成時及び電子署名検証時に分けて、夫々説明する。

#### 【0022】

まず、署名対象コンテンツ発行元のユーザ端末 2 と認証センターサーバ装置 1 との間において電子署名生成時に実行される電子署名依頼プログラム及び電子署名代行プログラムによる処理を、図 3 のフローチャート（電子署名依頼プログラム）、図 4 のフローチャート（電子署名代行プログラム）及び図 5 のシーケンス図を参照して説明する。

### 【 0 0 2 3 】

操作者が入力装置 2 5 を操作することによって所定のコマンドを入力すると、ユーザ端末 2 において、図 3 に示す電子署名依頼プログラムがスタートする。なお、このコマンドには、署名対象コンテンツのパス、鍵 I D 及びパスワードが、パラメータとして含まれている。

### 【 0 0 2 4 】

スタート後最初の S 0 1 において、電子署名依頼プログラムは、コマンドにてパラメータとして指定された鍵 I D 及びパスワードとともに、指定されたパスが示す署名対象コンテンツを取り込む。

### 【 0 0 2 5 】

次の S 0 2 では、電子署名依頼プログラムは、Digest 値計算部 2 2 2 を起動して、S 0 1 にて取り込んだ署名対象コンテンツの Digest 値の算出を命じる。

### 【 0 0 2 6 】

次の S 0 3 では、電子署名依頼プログラムは、S 0 1 にて取込んだ鍵 I D 及びパスワードと Digest 値計算部 2 2 2 によって算出された Digest 値とを含む電子署名生成依頼メッセージを、通信部 2 1 を経由して認証センターサーバ装置 1 へ送信する。その後、電子署名依頼プログラムは、S 0 4 において、S 0 3 にて送信した電子署名生成依頼メッセージに対する応答（即ち、後述する署名値）を認証センターサーバ装置 1 から受信するのを待つ。

### 【 0 0 2 7 】

認証センターサーバ装置 1 内においては、この電子署名作成依頼メッセージを受信すると、図 4 に示す電子署名代行プログラムがスタートする。スタート後最初の S 1 1 では、署名作成部 1 2 1 が、鍵管理部 1 2 3 を起動して、利用者端末 2 から受信した電子署名生成依頼メッセージに含まれる鍵 I D 及びパスワードの

組合せに対応する秘密鍵を、鍵格納庫 1 3 1 から検索させる。鍵管理部 1 2 3 は、そのような秘密鍵が鍵格納庫 1 3 1 内に存在する場合にはその秘密鍵を署名生成部 1 2 1 に応答するが、そのような秘密鍵が存在しない場合（鍵 ID とパスワードとが対応していない場合も含む）には、依頼元利用者端末 2 に対してエラーメッセージを送信する。

#### 【0 0 2 8】

秘密鍵を受け取った署名生成部 1 2 1 は、次の S 1 2 において、利用者端末 2 から受信した電子署名生成依頼メッセージに含まれる Digest 値を、鍵管理部 1 2 3 から受け取った秘密鍵によって暗号化することにより、電子署名の実体である「署名値」を生成する。

#### 【0 0 2 9】

次の S 1 3 では、署名生成部 1 2 1 は、S 1 2 にて生成した「署名値」を、通信部 1 1 を経由して依頼元利用者端末 2 へ送信する。

#### 【0 0 3 0】

依頼元利用者端末 2 内においては、電子署名依頼プログラムは、認証センターサーバ装置 1 から「署名値」を受信すると、処理を S 0 4 から S 0 5 へ進める。

#### 【0 0 3 1】

S 0 5 では、電子署名依頼プログラムは、コンテンツ構成部 2 2 1 を起動して、S 0 1 にて取り込んだ署名対象コンテンツに、同じく S 0 1 にて取り込んだ鍵 ID 及び S 0 4 にて認証センターサーバ装置 1 から受信した「署名値」を添付して、その全体を XML ファイルに格納することによって、電子署名付きコンテンツを構成する。このようにして構成された電子署名付きコンテンツは、必要に応じて暗号化され、電子メールに格納された状態でネットワーク N を通じて、若しくは、リムーバブル媒体に格納された状態で、その相手方へ送られる。

#### 【0 0 3 2】

次に、コンテンツの相手方のユーザ端末 2 と認証センターサーバ装置 1 との間において電子署名検証時に実行される電子署名依頼プログラム及び電子署名代行プログラムによる処理を、図 6 のフローチャート（電子署名依頼プログラム）、図 7 のフローチャート（電子署名代行プログラム）及び図 8 のシーケンス図を参



照して説明する。

#### 【0033】

操作者が入力装置 25 を操作することによって所定のコマンドを入力すると、ユーザ端末 2 において、図 6 に示す電子署名依頼プログラムがスタートする。なお、このコマンドには、電子署名付きコンテンツのパスが、パラメータとして含まれている。

#### 【0034】

スタート後最初の S 21 において、電子署名依頼プログラムは、コマンドにてパラメータとして指定されたパスが示す電子署名付きコンテンツを取り込む。

#### 【0035】

次の S 22 では、電子署名依頼プログラムは、コンテンツ構成部 221 を起動して、S 21 にて取り込んだ電子署名付きコンテンツから、署名対象コンテンツ、「署名値」及び鍵 ID を、夫々抽出する。

#### 【0036】

次の S 23 では、電子署名依頼プログラムは、Digest 値計算部 222 を起動して、S 22 にて抽出した署名対象コンテンツの Digest 値の算出を命じる。

#### 【0037】

次の S 24 では、電子署名依頼プログラムは、S 22 にて抽出した鍵 ID 及び「署名値」と Digest 値計算部 222 によって算出された Digest 値とを含む電子署名検証依頼メッセージを、通信部 21 を経由して認証センターサーバ装置 1 へ送信する。その後、電子署名依頼プログラムは、S 25 において、S 24 にて送信した電子署名検証依頼メッセージに対する応答（即ち、後述する検証結果）を認証センターサーバ装置 1 から受信するのを待つ。

#### 【0038】

認証センターサーバ装置 1 内においては、この電子署名検証依頼メッセージを受信すると、図 7 に示す電子署名代行プログラムがスタートする。スタート後最初の S 31 では、署名検証部 122 が、鍵管理部 123 を起動して、利用者端末 2 から受信した電子署名検証依頼メッセージに含まれる鍵 ID に対応する公開鍵を、鍵格納庫 131 から検索させる。鍵管理部 123 は、そのような公開鍵が鍵

格納庫 1 3 1 内に存在する場合にはその公開鍵を署名検証部 1 2 2 に応答するが、そのような公開鍵が存在しない場合には、依頼元利用者端末 2 に対してエラーメッセージを送信する。

#### 【 0 0 3 9 】

公開鍵を受け取った署名検証部 1 2 2 は、次の S 3 2 において、利用者端末 2 から受信した電子署名検証依頼メッセージに含まれる「署名値」を、鍵管理部 1 2 3 から受け取った公開鍵によって復号化する。

#### 【 0 0 4 0 】

次の S 3 3 では、署名検証部 1 2 2 は、S 3 2 にて復号化した「署名値」の内容が、利用者端末 2 から受信した電子署名検証依頼メッセージに含まれる Digest 値と一致するか否かを、チェックする。

#### 【 0 0 4 1 】

そして、両者が一致している場合は、Digest 値算出の元となった署名対象コンテンツが、その発行元によって電子署名依頼されたコンテンツ（即ち、その発行元の秘密鍵によって暗号化された Digest 値を算出する元となったコンテンツ）そのものであることが明らかであるので、署名検証部 1 2 2 は、S 3 4 において、署名検証結果：OK を、通信部 1 1 を経由して依頼元利用者端末 2 へ送信する。

#### 【 0 0 4 2 】

これに対して、両者が一致しなかった場合は、Digest 値算出の元となった署名対象コンテンツが、その発行元によって電子署名依頼されたコンテンツ（即ち、その発行元の秘密鍵によって暗号化された Digest 値を算出する元となったコンテンツ）そのものである保証がない（即ち、発行元の秘密鍵によって Digest 値が暗号化されてはいるが元々別のコンテンツである可能性がある、若しくは、発行元以外の者の秘密鍵によってそのコンテンツの Digest 値が暗号化された可能性がある）ので、署名検証部 1 2 2 は、S 3 5 において、署名検証結果：NG を、通信部 1 1 を経由して依頼元利用者端末 2 へ送信する。

#### 【 0 0 4 3 】

依頼元利用者端末 2 内においては、電子署名依頼プログラムは、認証センターサーバ装置 1 から何れかの署名検証結果を受信すると、処理を S 2 5 から S 2 6

へ進め、その署名検証結果をディスプレイ 24 上に表示する。

#### 【0044】

以上説明したように、本実施形態の電子署名システムは、電子署名の生成及び検証が各利用者端末 2 からネットワーク N を介して認証センターサーバ装置 1 に代行依頼される方式を採用するにも拘わらず、認証センターサーバ装置 1 内において実際に利用者の秘密鍵によって「署名値」として暗号化される情報（従って、認証センターサーバ装置 1 内において利用者の公開鍵によって「署名値」から復元される情報）は、署名対象コンテンツそのものではなく、その署名対象コンテンツから算出された Digest 値（ハッシュ値）でしかない。この Digest 値は一つのコンテンツから一意に生成されるが、その Digest 値に基づいて元のコンテンツの内容を再現することはできない。従って、この Digest 値を受け取り、また、Digest 値を復元した認証センターサーバ装置 1 は、署名対象コンテンツの内容を知ることができないが、間接的に、発行元によって電子署名作成依頼された署名対象コンテンツと相手方によって電子署名検証依頼された署名対象コンテンツとの異同を検証することができる。

#### 【0045】

##### 【発明の効果】

以上のように構成された本発明によると、電子署名の作成又は検証をネットワーク上のサーバ装置上において代行可能とすることによって、各個人の負担を軽減することができると同時に、署名対象電子情報そのものをサーバ装置において暗号化又は復号化することなく、電子署名として機能する署名値を作成することができるので、署名対象電子情報の内容がサーバ装置の運営者に知られることはない。

##### 【図面の簡単な説明】

【図 1】 本発明の実施の形態である電子署名システムのブロック図

【図 2】 鍵格納庫のデータ構成を論理的に示す表

【図 3】 電子署名生成時における電子署名依頼プログラムによる利用者端末内での処理内容を示すフローチャート

【図 4】 電子署名生成時における電子署名代行プログラムによる認証センター

サーバ装置内での処理内容を示すフローチャート

【図 5】 電子署名生成時における情報の流れを示すシーケンス図

【図 6】 電子署名検証時における電子署名依頼プログラムによる利用者端末内での処理内容を示すフローチャート

【図 7】 電子署名検証時における電子署名代行プログラムによる認証センターサーバ装置内での処理内容を示すフローチャート

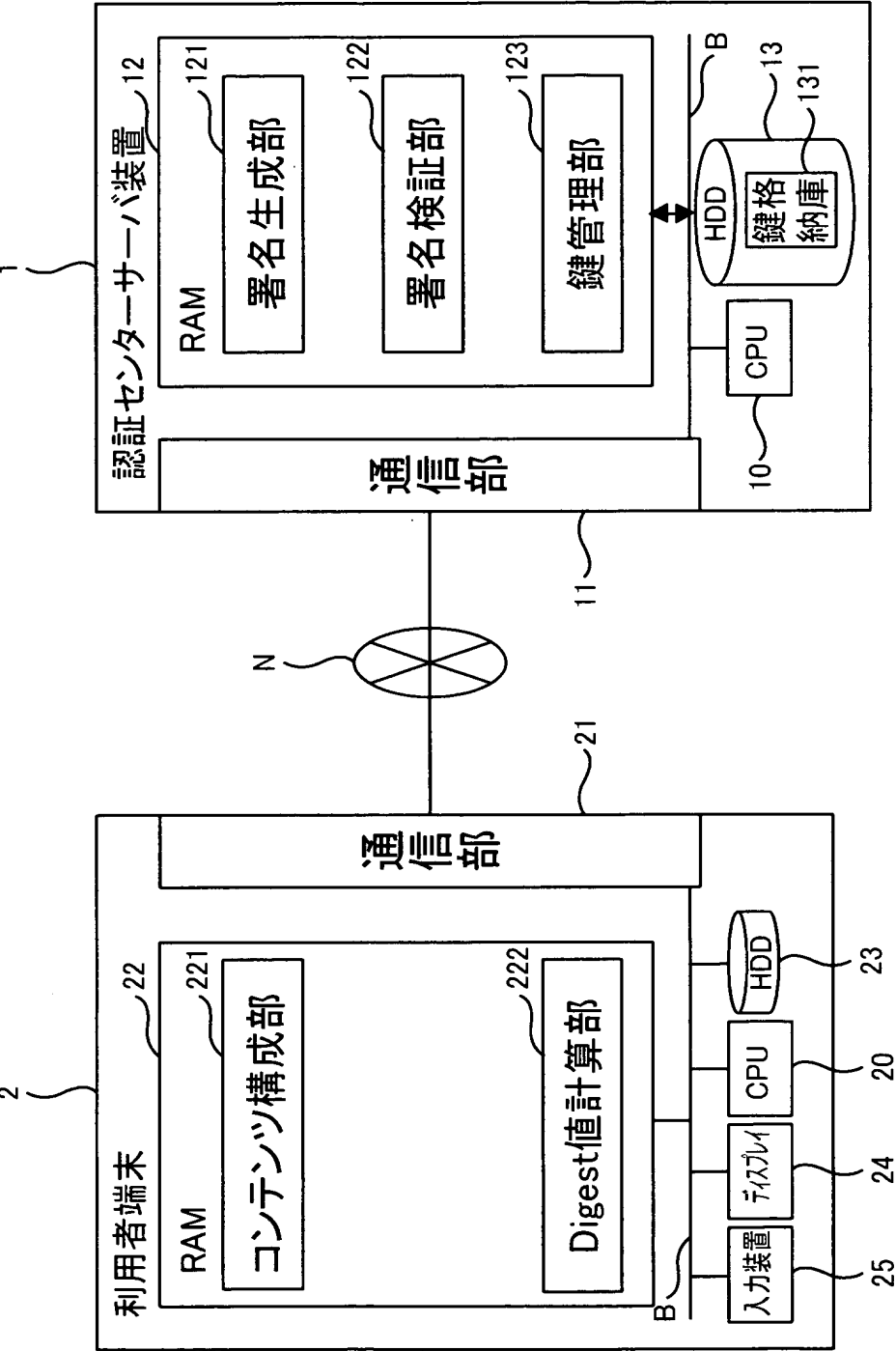
【図 8】 電子署名検証時における情報の流れを示すシーケンス図

【符号の説明】

- |       |             |
|-------|-------------|
| 1     | 認証センターサーバ装置 |
| 2     | 利用者端末       |
| 1 0   | C P U       |
| 1 1   | 通信部         |
| 1 2   | R A M       |
| 1 3   | H D D       |
| 2 0   | C P U       |
| 2 1   | 通信部         |
| 2 2   | R A M       |
| 2 3   | H D D       |
| 2 4   | ディスプレイ      |
| 2 5   | 入力装置        |
| 1 2 1 | 署名生成部       |
| 1 2 2 | 署名検証部       |
| 1 2 3 | 鍵管理部        |
| 1 3 1 | 鍵格納庫        |
| 2 2 1 | コンテンツ構成部    |
| 2 2 2 | Digest 値計算部 |

【書類名】 図面

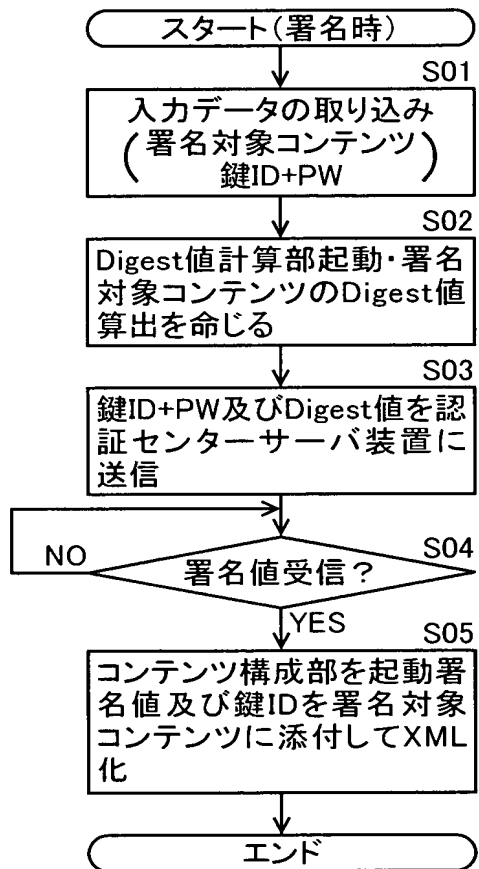
【図 1】



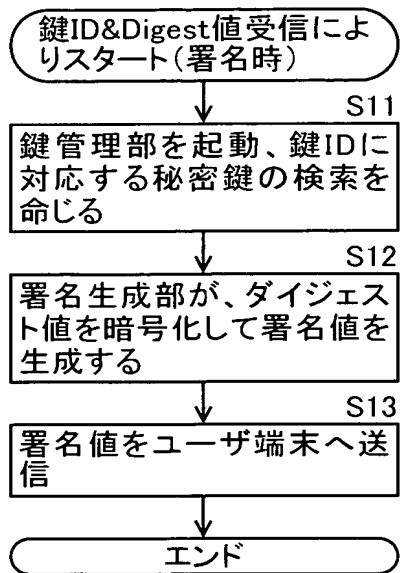
【図 2】

利用者A	鍵ID-A	PW-A	秘密鍵A	公開鍵A
利用者B	鍵ID-B	PW-B	秘密鍵B	公開鍵B
利用者C	鍵ID-C	PW-C	秘密鍵C	公開鍵C
利用者D	鍵ID-D	PW-D	秘密鍵D	公開鍵D
利用者E	鍵ID-E	PW-E	秘密鍵E	公開鍵E

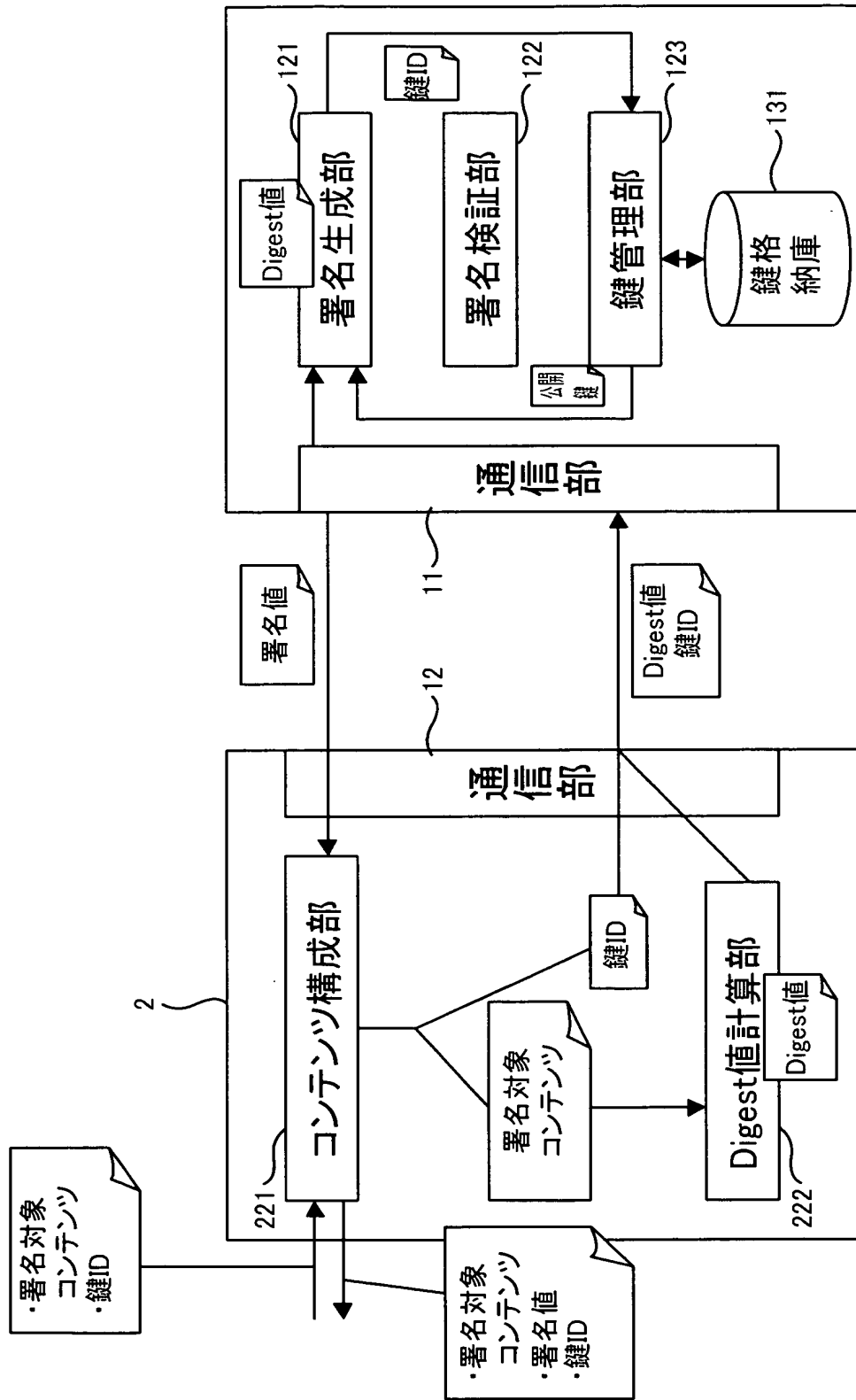
【図 3】



【図 4】

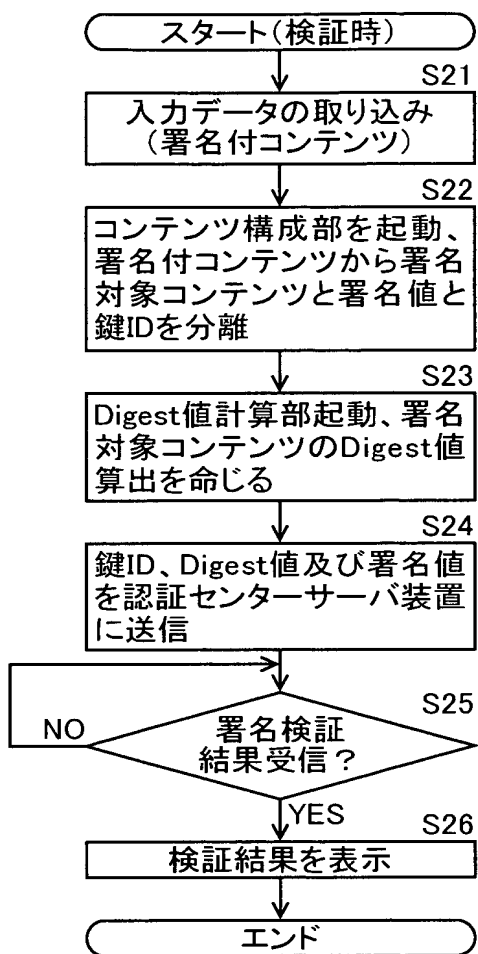


【図 5】

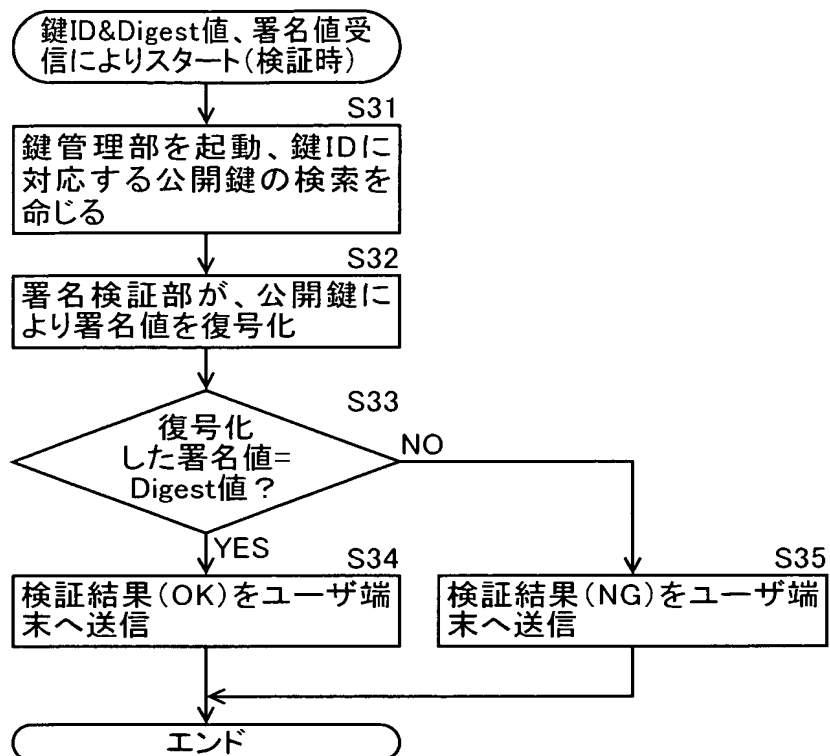




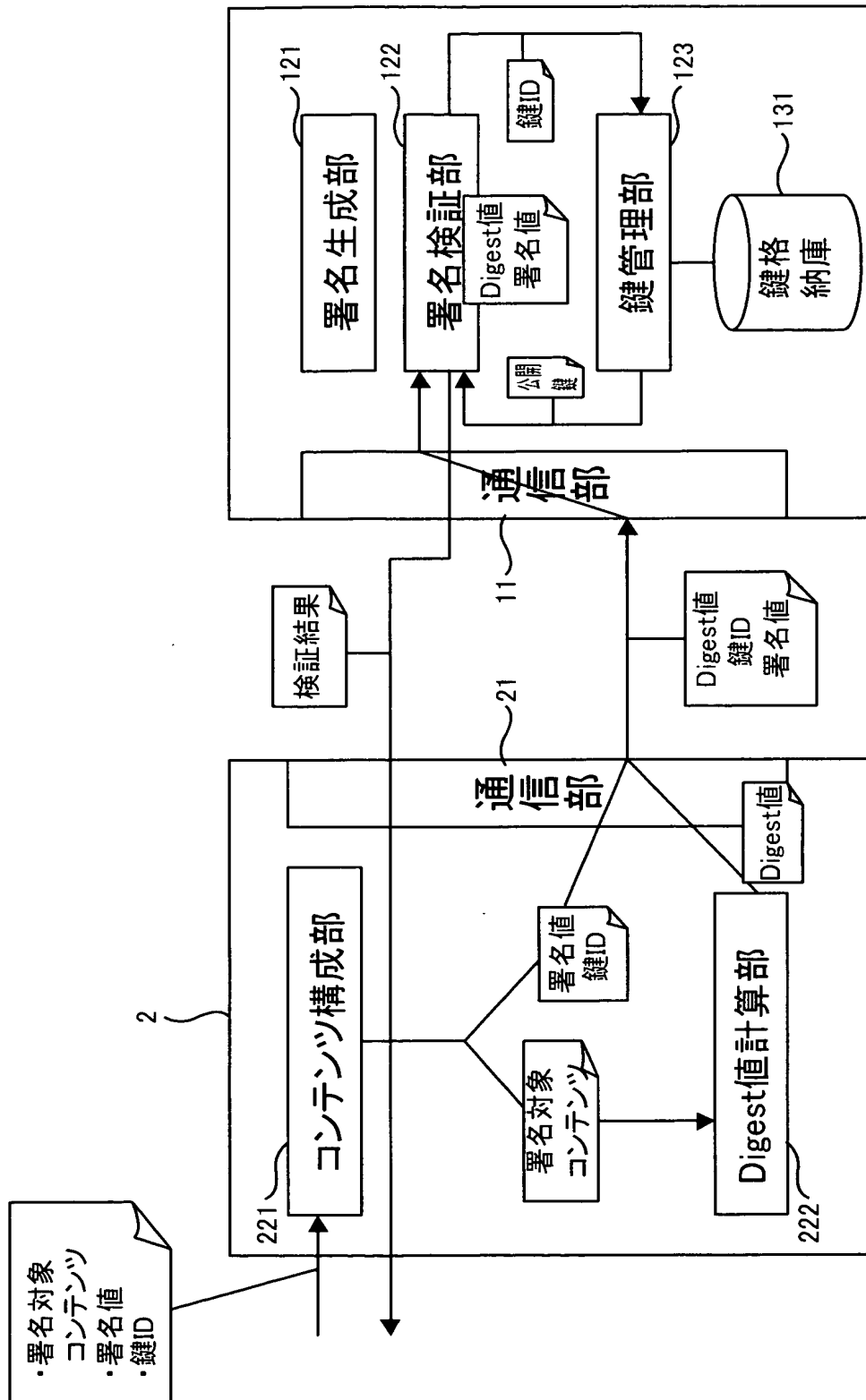
【図 6】



【図 7】



【図 8】



【書類名】 要約書

【要約】

【目的】 署名対象電子情報そのものをサーバ装置において暗号化又は復号化することなく電子署名の作成及び検証を行うことができる電子署名作成方法及び電子署名検証方法を、提供する。

【構成】

電子情報の発行元利用者の端末 2 は、コンテンツのDigest値を算出し、このDigest値及び発行元利用者の鍵IDを認証センターサーバ装置 1 へ送信する。認証センターサーバ装置 1 は、鍵IDに対応した秘密鍵を鍵格納庫 131 から検索し、この秘密鍵によってDigest値を暗号化することによって署名値を生成し、署名値を上記利用者端末 2 へ応答する。利用者端末 2 は、受信した署名値及び鍵IDを署名対象電子情報に添付することによって電子署名付きコンテンツを構成して、相手方へ発行する。相手方利用者の端末 2 は、電子署名付きコンテンツ中のコンテンツのDigest値を算出し、このDigest値、署名値及び添付鍵IDを認証センターサーバ装置 1 へ送信する。認証センターサーバ装置 1 は、鍵IDに対応した公開鍵を鍵格納庫 131 から検索し、この公開鍵によって署名値を復号化し、その復号結果がDigest値と一致するか否かを検証し、その検証結果を利用者端末 2 へ応答する。

【選択図】 図 1

認定・付加情報

特許出願の番号	特願 2 0 0 3 - 0 9 2 2 8 0
受付番号	5 0 3 0 0 5 2 0 6 9 0
書類名	特許願
担当官	第七担当上席 0 0 9 6
作成日	平成 1 5 年 4 月 7 日

< 認定情報・付加情報 >

【提出日】 平成15年 3月28日

次頁無

特願 2 0 0 3 - 0 9 2 2 8 0

出 願 人 履 歴 情 報

識別番号

[ 0 0 0 0 0 5 2 2 3 ]

1. 変更年月日

1 9 9 6 年 3 月 2 6 日

[変更理由]

住所変更

住 所

神奈川県川崎市中原区上小田中 4 丁目 1 番 1 号

氏 名

富士通株式会社